International Journal on Management Education & Emerging Technology
ISSN: 2583-9438

A Case Study About Self-Interest Over Social Responsibility Of An Individual: The Context Of Ethical Egoism Among Data Hackers

Ma. Veronica Cabie[1], Raymond Cuevas[2], Maureen Dulay[3], Jay Manog[4], John Rick Medina[5], Robbylyn Soliven[6], Jonathan Sudio[7]
[1,2,3,4,5,6,7] *Polytechnic University of the Philippines – Parañaque Campus*

Abstract

This study aimed to understand the common misconception that data hackers are solely concerned with their self-interest and determine whether they put self-interest ahead of societal duty. Interviews and observations were utilized in two Discord communities focusing on White hat hackers to identify the motivation of the data hackers. Based on the outcome of the study, social responsibility is typical in white hat hackers. It also showed that ethical hacker members did not tolerate unethical behavior inside the Discord communities. The study also highlights a different kind of motivation including personal interest, creativity, and a social responsibility to online security. The results showed that data hackers are not only motivated by their self-interest; this study illustrates that a substantial number of hackers are motivated by social responsibility, especially white hat hackers.

Article Info

Keywords:
Cybersecurity, Motivation, Ethical hacking, Hacker types, Hacker communities

Date of Submission: 17/12/2023
Date of Review: 25/02/2024
Date of Acceptance: 3/03/2024
IJMEET / Volume 2, Issue 1, 2024

INTRODUCTION

As society maneuvers itself in the rapid advancement of technology, IT practitioners have become important forces in the efforts of strengthening and protecting one's cybersecurity and data privacy which brings people's attention to their current behaviors and activities especially when it comes to data hackers who are related in this aspect.

In general, motivation is described as the driving force behind a person's action and in the study of Cayubit et al. (2017), they identified three factors perceived by hackers for their reason in hacking which is (1) superiority wherein they are motivated by a sense of accomplishment, (2) exploitative wherein it is seen as a way to take hold of opportunities to exploit or benefit from others, and (3) opportunistic in which hacking is seen as an opportunity to satisfy their immediate needs such as curiosity, fun, and attention from others. From the second factor alone, hackers can be said to be egoistic as the purposes under this factor includes expanding their experience and connections to be part of a group, taking advantage of the vulnerable, and gaining free access to products and services to bypass payment obligations (Cayubit et al., 2017) which can be seen as actions done for one's benefit.

On another note, data hackers have also been associated with dishonorable and unprincipled actions as cybercrimes such as unauthorized hacking, data breaches, ransomware, and others came to rise. This is despite the legislation, laws, and regulations implemented by countries to penalize offenders. Examples of such laws include the Cybercrime Prevention Act and Data Privacy Act in the Philippines, Computer Fraud and Abuse Act in the United States, and lastly, the Penal Code and the Act on Prohibition of Unauthorized Computer Access in Japan. According to Curtis & Oxburgh (2023), it is due to the sense of anonymity and distance from the real world that online offenders are likely to become repeat offenders as they feel less burdened for their behaviors towards victims and encounter few or less consequences for their actions.

But contrary to negative beliefs about hackers, it was also stated under the factor of superiority that hackers view hacking in a positive light as they see it as means to further their knowledge to aid others which in return lets them enjoy a sense of personal fulfilment described by a boost in their self-confidence and self- esteem for being able to demonstrate their care for others (Cabuyit et al., 2017). This shows that as hackers, they are also capable of thinking about others.

In addition, albeit one embraces the right to behave in one's self-interest under ethical egoism; this does not imply that a person does not care towards others, it only means that they prioritize their self rather than being fixated on another's life, although it may overlook other people's want in favor of their own (Hassan, 2019). Furthermore, Prasad (2014) stated that there exist white hat hackers who practice ethical hacking and help others to improve their security flaws. Thus, this paper would like to explore the motivations and actions of data hackers in circumstances involving self-interest and social responsibility from an ethical egoism standpoint to grasp the intricacies among them.

Types of Data Hackers and Hacking

Data hacking is an act of gaining unauthorized access to a computer system or account through the use of digital devices and networks for various reasons (Prasad, 2014). While the people who perform this act are called data hackers.

The number of cybercrimes is increasing each year (International Telecommunication Union, 2019) and the most common type of cybercrime is information security failures or data breaches. According to the study of Hammouchi, Chergi, Mezzour, Ghogho, and El Koutbi (2019) among the records of data breaches from the year 2005 to 2018, the hack breach method holds the most number of breaches recorded. Considering the huge number of data hackers' bad records, people are stereotyping these hackers as unethical individuals who commit cybercrimes. However, not all hackers are classified as criminals as a lot of people would think (Hoath & Mulhall, 1998, as cited in Cayubit, 2017), given that there are types of data hackers that help organizations to protect their computer system against cybercrimes. These types of hackers are called white hat hackers, who do not have malicious intent and follow ethical hacking practices.

Cybersecurity experts have studied the different motivations, hacking techniques, and objectives of hackers. This way they are able to differentiate hackers into their typologies (Chng et al., 2022). There are diverse types of hackers now. But the most commonly known categories are white hats, black hats, and grey hats (Nasr et al., 2018).

Hackers that are hired to examine a system or software for vulnerabilities which can help the big companies or organizations to strengthen their cyber security are called white hat hackers. White hats' techniques may be similar to black hats', but their intentions are far from being the same because white hat hackers work accordingly with the law by legally protecting their clients from cyber-attacks (Jaquet-Chiffelle & Loi, 2020). Contrary to white hats, black hat hackers are the so-called "bad guys" whose values are aligned to illegal activities. They hack into computer systems without the owner's consent and are driven by their malicious intent and personal gain (Jaquet-Chiffelle & Loi, 2020).

Gray hat hackers stand in between white hats and black hats because they usually hack without malicious intent, however, their ways to achieve their objectives may include illegal compliance with the law. For example, they hack into a system to raise awareness about its vulnerabilities. But instead of communicating it privately to the system's owner, they mostly let them know publicly, and they sometimes upload data that they gained from hacking (Jaquet-Chiffelle & Loi, 2020).

There are also red hat hackers who share the same goal as white hat hackers of stopping all upcoming attacks by black hat hackers. Red hat hackers are seen as vigilantes since they attempt to punish black hat by destroying its computers and resources after breaking into the black hat itself (Filiol, Mercaldo, & Santone, 2021).

Digging deeper into some of the more detailed types of data hackers, Chng et al. (2022) have listed thirteen hacker types and seven unique motivations in their article titled Hacker types, Motivations and Strategies: A Comprehensive Framework. This table is a summary of the hacker types, their definition, and the underlying motivations for their hacking.

Table 1: Definition and Motivation of Different Types of Hackers

Hacker Types	Definition	Motivations
Novices	Hackers with little experience who basically depend on web toolkits	Curiosity, notoriety, and recreation
Cyberpunks	Low to medium-skilled hackers who just enjoys causing mayhems	Financial, notoriety, revenge, and recreation
Insiders	Dissatisfied present or former workers who abuse their access to attain their intended objectives.	Financial, revenge, and ideology
Old Guards	Hackers who engage in non-malicious hacking activities, but disregard personal privacy	Curiosity, notoriety, recreation, and ideology
Professionals	Highly proficient hackers who use their skills to advance their criminal empire or offer their services.	Financial, and revenge
Hacktivists	Hackers employ their technical expertise to advance their political motives or leverage the internet as a tool for political transformation.	Notoriety, revenge, recreation, and ideology
Nation States	Proficiently experienced hackers, who are either directly or indirectly employed by a government, aim to destabilize, disrupt, and dismantle the nation or government's network system through their exceptional skills.	Financial, revenge, and ideology
Students	Hackers who engage in hacking activities solely for the purpose of acquiring knowledge, without any malicious intent.	Curiosity
Petty Thieves	Criminals who transition their operations online, leveraging their low to medium hacking skills.	Financial, and revenge
Digital Pirates	Individuals who have copyrighted materials and partake in the unauthorized replication, dissemination, acquisition, or trade of it.	Financial
Online Sex Offenders	Individuals who use the internet for the purpose of engaging in sexually inappropriate behavior with minors.	Sexual Impulses
Crowdsourcers	Crowdsources are people who unite to address a challenge, frequently employing questionable approaches or pursuing uncertain objectives.	Notoriety, revenge, recreation, and ideology
Crime Facilitators	Individuals who equip cybercriminals with essential tools and expertise, empowering them to execute intricate attacks.	Financial

excerpt from Chng et al. (2022) "Hacker types, Motivations and Strategies: A Comprehensive Framework" Source: https://doi.org/10.1016/j.chbr.2022.100167

Self-interest and Well-being

In ethical egoism, an individual's basis for decision would be their self-interest, taking advantage of a situation regardless of the effect on others. In his book of ethical theories, Quinn (2020) notes that under ethical egoism, self-interest relates with the "maximum long-term benefit" (p.186) of a person. It was stated that a person prioritizing self-interest can be seen as recognizing the need to focus on their well-being as it is a person's natural inclination to do what is best for themselves. But he also argues that this idea ignores the fact that natural inclinations do not always align with a person's best interest and acting on self-interest does not always promote long-term benefits. According to Crocker et al. 's (2017), they did not locate recent studies demonstrating that selfish motivation is favorable for an individual's psychological well-being, physical health, or relationships although they have said that this finding may only suggest a lack of interest on such research subjects. They have also found that people who do not genuinely care for others and their relationship with them seem to be immune to the negative effects of selfishness, such as narcissists. In their literature, selfish motivation is linked to unfavorable relationships, physical health, and psychological well-being. Conversely, those with high traits of narcissism appear content with their relationships and report high life satisfaction, well-being, and self-esteem.

As mentioned before, data hackers have different interests in mind when hacking and can lead to differing cases for an individual. One such case is being criminalized and penalized when violating existing implemented laws regarding cyber activity by countries. In others, it is a way to further broaden their knowledge as security experts. Following Albert Bandura's social learning theory, people can acquire knowledge and skills through observation and modelling. This theory encompasses various mechanisms, including peer influence. According to Bandura, when influential individuals within a group adopt a new fashion style, others in the group tend to observe and imitate it. A study conducted by Nasr et al (2018) reveals a correlation between individuals engaged in online hacking communities and their actual hacking identity, similar in the way that social learning theory operates. It is worth noting that hackers within learning communities often utilize their skills for the benefit and security of the community.

In Votipka et al. 's (2018) paper, hackers from bug bounty services tend to have an advantage when it comes to experience compared to testers from companies due to their involvement in a variety of programs and vulnerabilities from their employments, exercises, and communities which they have identified as a critical factor in vulnerability discovery which is an important aspect in cybersecurity. It was also stated that the hackers gave higher self-reported skill ratings compared to the testers which they believe reflects the testers tendency to have less faith in their ability to identify security flaws.

Social Responsibility in the Digital Age

Being accountable for one's action and acting in a manner that provides a positive impact on society is a means of social responsibility, Akre and Komrelliwar (2023). An organization's social responsibility includes taking responsibility for the impact of its choices and actions have on society and the environment. It additionally includes maintaining ethical behavior, sustainable development, stakeholder expectations, legal compliance, transparency, and integration across the whole organization (ISO 26000).

Nowadays, moral dilemmas are often presented digitally, i.e., relevant information is presented through, and decisions are made on a technological device (Barque-Duran et al., 2017). In the field of cybersecurity, social responsibility is crucial. The study of Ponemon Institute about Cost of a Data Breach 2021 finds that appropriate cybersecurity contributes to the prevention of data breaches, which can have negative impacts on people and businesses. Strong security measures lower the possibility of data compromise and illegal access. Social responsibility also guides the ethical decision-making within the security field. As per the research conducted by Bada, Sasse and Nurse (2015). It evidently highlights how important social responsibility is in directing moral judgments in the field of cybersecurity. In this context, social responsibility refers to the moral duties that people and organizations must think about how their actions will affect society, including concerns about privacy, trust, and responsible technology use which is needed in today's time in the world of cybersecurity.

Ethical hackers play a major role in enhancing and safeguarding cybersecurity and identifying system vulnerabilities. To make sure they have permission to access the system, their hacking activities need to be approved. Ensuring the confidentiality of sensitive information is their social responsibility as they evaluate

the system. It is their responsibility to develop a safer and more secure digital environment. Ethics-based hacking can be classified as a security assessment, a type of training, and an examination of the information technology environment. An authorized hack reveals the dangers that exist in an information technology environment and actions that can be taken to either accept or reduce risks (Sahare, Naik, & Khandey, 2014).

Self-interest and Social Responsibility in Ethical Egoism

According to ethical egoism, people tend to follow their own goals first; however, considering how this concept relates to social responsibility, it shows a more complicated connection between self-centered hobbies and social responsibility. This case discusses the ethical egoism of hackers and the viable and societal effects that could result from it.

Despite its recognition as self-centered, ethical egoism does not always negate the popularity of societal obligations. Individuals committing to ethical egoism might also realize that some social actions enhance their well-being and prosperity, agreeing that ethical activity can indirectly serve self-hobby (Nasr et al, 2018). This factor of view attracts interest in the technicalities of ethical egoism, which holds that people can behave morally righteously if they pursue their dreams. Hacker types, motivations, and strategies gives light on potential conflicts and emphasize the distinct characteristics of data hackers (Chng et al., 2022). Conflicts may arise when the moral concerns of proper hacking techniques clash with their desire for self-interest, such as fame or wealth. Such conflicts may have far-reaching implications for privacy, data security, and public trust in the security of digital systems.

The study by Votipka et al. (2018) compared testers and hackers in finding software vulnerabilities and when considering the implications of a conflict, hackers identify software flaws by stressing the potential societal consequences. Due to a conflict between their self-interest and societal obligation, data hackers may exploit cybersecurity faults, risking the integrity of digital systems and exposing vulnerabilities that attackers can exploit.

For example, a financial hacker can plan a sophisticated data breach that compromises customer information for personal gain. This would go against the larger social responsibility to protect people's privacy and welfare. A real-life scenario is the 2016 COMELEC breach in the Philippines, according to Department of Justice (2017) a group of Hackers known as Lulzsec Philippines gained unauthorized access to the personal information of at least 70 million registered voters through a breach in the COMELEC database which occurred after Anonymous Philippines vandalized the organization's website on March 27, 2016. Another possibility is that hackers are spreading fake news for political or personal gain, swaying public opinion, and undermining the duty of accurate information in a democracy. Even though hackers use ransomware to threaten companies to put their interests first, they can, however, do so for those whose crisis emphasizes the social responsibility of protecting vital policies for society.

DATA AND METHODOLOGY

Case studies are comprehensive studies of specific subjects, things, or situations that are helpful in evaluating specific cases and allow researchers to learn much more about a certain individual or group of individuals (MSEd, 2024). In this way, the researchers observed and interviewed to better understand the motivations behind hackers' moral behavior in data security while hovering the balance between self-interest and social responsibility.

The researchers focused on white hat hackers and searched for two online communities that focuses on the topic of data hacking and have decided to join online communities for cybersecurity which is the closest relevant community that can be found by the researchers in Discord, an online voice, video, and text communication service. For 4-5 days, an observation on the online activities within the group was done to gather the data that will be used to assess the motivation of a data hacker in data hacking. Observations ended as soon as the conversation topics became repetitive. Afterwards, an interview was conducted.

RESULTS AND DISCUSSION

Results

Presented below is the description of the online community groups selected during the observation period and the respective tables displaying the responses gathered from the interviews.

The Community

The first community of hackers had a collaborative environment where they helped each other to improve. The platform they use to engage in ethical hacking is "Hack the Box" where members are learning penetration testing and ethical hacking skills. Skilled members of the Discord server demonstrated openness and enthusiasm to aid beginners in the hacking field they are not familiar with. The members are also open to hacking each other by asking permission to hack each other. The hackers consider themselves as ethical hackers or white hat hackers and stated that they are driven by a sense of social responsibility. In contrast to their counterparts in black hats, white hats wanted to contribute instead of attacking other people, they wanted to use their knowledge to penetrate by protecting the company and organization. They also did not tolerate unethical behavior inside the server; they automatically responded to prevent such acts.

In the second community, the researchers have observed a relatively low level of overall activity. While the community exists, it seems that only a select few members engage daily. Interestingly, the discussions within the servers appear to deviate from the expected focus on ethical hacking. Instead, the predominant topics include random banter, meme exchanges, requests for programming homework assistance, and occasional disputes between longstanding members and disruptive trolls.

Interview Responses

Table 2: Response for Question No.1

Q1	**Can you share your motivation for engaging in White Hat hacking activities? Is it driven more by personal interest or a sense of social responsibility?**
ANSW	"Social responsibility, and almost ruining my life in 2022" "Ex snitched on me for petty computer crimes and snitched on me for some swats I did (i wasnt a casual swatter like someone who just goes around swatting people. im not like that). When that happened I had TBI overturn my case to FBI and with the petty shit and the swatting together they were wanting to charge me with like 6 felonys, and I think they said 12 Years, I took a guilty plea and got 8 months probation with supervised computer access. Was unable to use a computer unless it was monitored was such bullshit. and I went to a camp at a college and I realised I was alot better than my peers, and decided that I wanted to contribute instead of attacking everything, and just being offensive, I could use the offensive knowledge I know to protect orgs and companys. Realising that mistakes follow you throughout your life is probably the biggest lesson I've learned as Im ashamed for my idiotacy in my past but I've learned to put it behind me and attempt to do what I can to help others that are interested in the only thing I can do (Anything Computer Related Essentially.). Now I tutor CIT Students, and am now employed by my college." "Anyway, I came back from that camp different and realised I needed to be constructive and helping and making a difference in what I can instead of breaking it all down" "Proceeding that my life has been so much better. My mental health is extremely better, and I was able to get off probation early (only 2 months early lol) and start college as the youngest person enrolled as a real student (edited)" "I realised I could help others, and I actually enjoyed doing it. College starts back tomorrow and I can't wait to see my CIT students and go to my Security+ class" "(that experience also made me take academics seriously I never before took them serious until after)"
	"Definitely kinda both cause it's more like familial responsibility with a mix of personal interest (edited)"
	Personal Interest
	"Money + Creativity"
	Personal Interest
	"So you know doing this whitehat hacking for me is like this awesome mix of personal interest and feeling a bit like an internet hero. I've always been that tech geek who loves pulling things apart just to see how they work, and hacking lets me do that." "You know with everything going digital we are more likely do this not for ourselves but for the others to. So for me its a mix mix between personal curiosity and sense of duty for the community online."

Among the six respondents, one responded social responsibility as their motivation for engaging in white hat hacking activities, one answered money and creativity, two of them answered personal interest, while the other two reasoned that they both have a sense of self-interest and social responsibility. It can be observed here that although most of the respondents are motivated by self-interest, they

still think about their social obligations and the adverse effects of their actions towards society. It is also evident during the observations that the members of the groups showed enthusiasm in teaching beginners about ethical hacking and discourages the act of unethical hacking behaviors.

Table 1: Response for Question No.2

Q2	**Have you encountered situations where your ethical principles clashed with the goals of the White Hat hacking community? How did you navigate such conflicts?**
ANSW	"Not really, white hat hacking embraces ethical principles. Which is respectable. There is hardly any conflict."
	"No I haven't"
	"Maybe"
	"Yeah, it happens. There are times when the community aims for one thing, but my want is slightly elsewhere. usually I take a step back and weigh the pros and cons and if it doesn't align with my principles I just opt out. Personal integrity over everything, you know? Gotta stay true to yourself in this digital playground sometimes its really risky to move."

In the second question, among the four respondents, two of them said that they have not encountered such conflicts, one is uncertain, and there is one who said that it does happen and that he would usually weigh the pros and cons when the aims of the community do not align with his principles. This shows that conflicts between self-interest and social responsibility rarely happens in white hat hacking communities and when it does, a hacker would consider the consequences of their actions whether it does them good or bad or aligns with their principles.

Table 4: Response for Question No.3

Q3	**In your opinion, how does the White Hat hacking community contribute to the broader concept of social responsibility in the digital landscape**
ANSW	"They take there responsibility very well, they prevent the bad thing from happening" "And much better to take care of every piece of information"
	"It helps protect the community and develop a sense of security and creativity."
	"Just like what ive said earlier we act like guards to maintain the secure space for everyone. For me its a personal responsibility nothing more. You might ask what do we gain doing this and the answer to that is most of us just want to make the internet secure for users like you."

For the last question, only three people shared their views, and all three of them showed awareness of their responsibilities and importance in cyber security and protecting data responsibility. One of the three specifically stated that most of them do not gain anything from doing so and does it just to secure the online community.

Discussion

The researchers explored the complexity of ethical egoism in the domain of data hackers. Ethical egoism, when applied to data hackers, proposes a preference for self-interest over social responsibility. However, it is crucial to acknowledge that the self-centered nature inherent in ethical egoism does not necessarily clash with an individual's social responsibility. Interestingly, these two opposing forces can align, as societal obligations often align with actions that promote an individual's long-term benefits.

From the results, several key motivations were identified including personal interest, social responsibility, a combination of the two, money and creativity, as well as curiosity. Personal interest as a motivation conforms with the idea of ethical egoism in which people tend to prioritize personal goals first. Meanwhile, social responsibility as a motivation can be reflected in Cayubit et al.'s (2017) study wherein hackers are described to be motivated by the sense of accomplishment brought by the increase in confidence, esteem, ego, and pride from being able to care for others. On the other hand, money and curiosity as motivations align with Chng et al.'s (2022) framework for hacker definitions, motivations, and types. As what is seen, although hacker motivations could be self-centered, there exists motivations that lead them to also meet societal expectations which reflects Hoath and Mulhall's belief that not all hacking motivations are inappropriate. Furthermore, it was also shown that hackers themselves are aware of their importance and responsibility as practitioners in the

field and can identify and differentiate which behaviors or actions could benefit them or not which can be attributed to their exposure to such practices as associated with the explanation under the social learning theory.

CONCLUSION

This study puts forward the idea that hackers are not solely driven by self-interest, highlighting that a portion of hackers are motivated by a sense of social responsibility. However, it is important to recognize that this association between hacking and social responsibility does not apply universally to all hacker types as results are specific to the observed online groups. Additionally, the answers given during the interview may have been socially desirable responses. The limitations also include the fact that the observation period was short and that it focused on one kind of hacker only. Therefore, the researchers would like to recommend interested future researchers to aim at other types of hackers as subjects for their study and to extend the observation period for more diverse data.

REFERENCES

Akre, A., Komrelliwar,O. (2023). View of impact of social responsibility in today's youth. https://journal.hmjournals.com/index.php/JSRTH/article/view/2095/2159?fbclid=IwAR3Mhx8cIPzB S3e9IjvTeC-1Nx7onhqJ76TlVnhfFb6RBdWK3g1Lh02Roio Bada, M. (2019, January 9). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. arXiv.org. https://arxiv.org/abs/1901.02672

Barqué-Duran, A., Pothos, E. M., Hampton, J. A., & Yearsley, J. M. (2017). Contemporary morality: Moral judgments in digital contexts. Computers in Human Behavior, 75, 184–193. https://doi.org/10.1016/j.chb.2017.05.020

Cayubit, R.F.O., Rebolledo, K.M., Kintanar, R.G.A. et al. (2017). A Cyber Phenomenon: A Q-Analysis on the Motivation of Computer Hackers. Psychol Stud. doi: https://doi.org/10.1007/s12646-017-0423-9. https://www.academia.edu/87753408/A_Cyber_Phenomenon_A_Q_Analysis_on_the_Motivation_of _Computer_Hackers?sm=b Charles, Z. (2022). Cyber Security and Philosophy: An Intersection. Retrieved from https://inds.uccs.edu/sites/g/files/kjihxj2421/files/2022-06/Philosophy-Charles-Final-Paper.pdf.

Chng, S., Lü, H., Kumar, A., & Yau, D. K. Y. (2022). Hacker types, motivations and strategies: A comprehensive framework. Computers in Human Behavior Reports, 5, 100167. https://doi.org/10.1016/j.chbr.2022.100167

Crocker, J., Canevello, A., Brown, A. (2017). Social Motivation: Costs and Benefits of Selfishness and Otherishness. Annual Review of Psychology, 68, 299-325. https://doi.org/10.1146/annurev-psych- 010416-044145

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. The Police Journal, 96(4), 573-592. https://doi.org/10.1177/0032258X221107584

Cybercrime Prevention Act of 2012 (2012). https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html Data Privacy Act of 2012 (2012). https://lawphil.net/statutes/repacts/ra2012/ra_10173_2012.html

Department of Justice (2017). OOC REPORT FINAL. Retrieved from https://doj.gov.ph/files/OOC/OOC%20REPORT%20FINAL.pdf

Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical Dilemmas and Privacy Issues in Emerging Technologies: A review. Sensors, 23(3), 1151. https://doi.org/10.3390/s23031151

Filiol, É., Mercaldo, F., & Santone, A. (2021). A method for automatic penetration testing and mitigation: a red hat approach. Procedia Computer Science, 192, 2039–2046. https://doi.org/10.1016/j.procs.2021.08.210.

Hammouchi, H., Chergi, O., Mezzour, G., Ghogho, M., El Koutbi, M. (2019). Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches Over Time. Procedia Computer Science, 151, 1004–1009. https://doi.org/10.1016/j.procs.2019.04.141

Hassan, P. (2019). Virtue & The Problem of Egoism in Schopenhauer's Moral Philosophy. Retrieved from https://philpapers.org/archive/HASVAT.pdf

Ho, B. (2017). A Defense of Egoism. Retrieved from https://philpapers.org/archive/BACADO-2.pdf. International Telecommunication Union — Statistics. (2023). Statistics (itu.int)

ISO - ISO 26000 — Social responsibility. (2021, October 15). ISO. https://www.iso.org/iso-26000- social-responsibility.html

Japan - Octopus Cybercrime Community - www.coe.int. (n.d.). Octopus Cybercrime Community. https://www.coe.int/en/web/octopus/-/japan_legislation

Jaquet-Chiffelle, D. 0., & Loi, M. (2020). Ethical and Unethical Hacking. Chapter 9. https://doi.org/10.1007/978-3-030-29053-5_9

Kodapanakkal, R. I., Brandt, M. J., Kogler, C., & van Beest, I. (2020). The impact of online hate speech on social media: A systematic review. Computers in Human Behavior, 107, 106303. https://doi.org/10.1016/j.chb.2020.106303

MSEd, K. C. (2024b, January 18). What is a case study? Verywell Mind. https://www.verywellmind.com/how-to-write-a-psychology-case-study-2795722

NACDL - Computer Fraud and Abuse Act (CFAA). (n.d.). NACDL - National Association of Criminal Defense Lawyers. https://www.nacdl.org/Landing/ComputerFraudandAbuseAct

Nasr, E. (2018). An analytical approach to psychological behavior of hackers' motives. Academia. https://www.academia.edu/27358059/An_Analytical_Approach_to_Psychological_Behavior_of_Hac

kers_Motives Nobis, N. (2019). 1000-Word PHILOSOPHY An Introductory Anthology. Retrieved from https://philpapers.org/archive/NOBEE.pdf

Prasad, S. T. (2014). Ethical Hacking and Types of Hackers. Retrieved from https://www.ijetcse.com/admin/uploads/Ethical%20Hacking%20and%20Types%20of%20Hackers_16

05787993.pdf

Quinn, M. (2020). Ethics for the information age (8th ed.). Pearson

Owen, K. (2016). Motivation and Demotivation of Hacker Activities – A Contextual Approach. Owen_Kenneth_D_201604_PhD -Business-Admin.pdf (mcmaster.ca)

Sahare, B., Naik, A., & Khandey, S. (2014). Study of ethical hacking. Int. J. Comput. Sci. Trends Technol, 2(4), 6-10.

Sinha, S., & Arora, Y. (2020). Ethical Hacking:The story of a white hat hacker. Social Science Research Network. https://doi.org/10.2139/ssrn.3670801

Votipka, D., Stevens, R., Redmiles, E., Hu, J., and Mazurek, M. (2018). Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes. 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, (pp. 374-391). Institute of Electrical and Electronics Engineers. doi: 10.1109/SP.2018.00003. https://ieeexplore.ieee.org/abstract/document/8418614